TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 293, Number 2, February 1986

THE DISTRIBUTION OF SOLUTIONS TO EQUATIONS OVER FINITE FIELDS

BY

TODD COCHRANE[1]

ABSTRACT. Let $\mathbf{F}_q$ be the finite field in $q = p^f$ elements, $\underline{F}(\underline{x})$ be a k-tuple of polynomials in $\mathbf{F}_q[x_1, \dots, x_n]$, V be the set of points in $\mathbf{F}_q^n$ satisfying $\underline{F}(\underline{x}) = \underline{0}$ and S, T be any subsets of $\mathbf{F}_q^n$. Set $\phi(V, \underline{0}) = |V| - q^{n-k}$,

$$\phi(V, \underline{y}) = \sum_{\underline{x} \in V} e\left(\frac{2\pi i}{p} \operatorname{Tr}(\underline{x} \cdot \underline{y})\right) \quad \text{for } \underline{y} \neq \underline{0},$$

and $\Phi(V) = \max_{\underline{y}} |\phi(V, \underline{y})|$. We use finite Fourier series to show that $(S + T) \cap V$ is nonempty if $|S||T| > \Phi^2(V) q^{2k}$. In case $q = p$ we deduce from this, for example, that if C is a convex subset of $\mathbf{R}^n$ symmetric about a point in $\mathbf{Z}^n$, of diameter $< 2p$ (with respect to the sup norm), and $\operatorname{Vol}(C) > 2^{2n}\Phi(V)p^k$, then C contains a solution of $\underline{F}(\underline{x}) \equiv \underline{0} \pmod{p}$.

We also show that if B is a box of points in $\mathbf{F}_q^n$ not contained in any $(n-1)$-dimensional subspace and $|B| > 4 \cdot 2^{n/f}\Phi(V)q^k$, then $B \cap V$ contains n linearly independent points.

1. Introduction. Let $\mathbf{F}_q$ be the finite field in $q = p^f$ elements where p is a prime. Let $\underline{F}(\underline{x}) = (f_1(\underline{x}), \dots, f_k(\underline{x}))$ be a k-tuple of polynomials in $\mathbf{F}_q[x_1, \dots, x_n]$ and $V = V(\underline{F})$ be the algebraic subset of $\mathbf{F}_q^n$ defined by the equations

$$f_1(\underline{x}) = \cdots = f_k(\underline{x}) = 0. \tag{1.1}$$

Considerable attention has been given to the problem of finding solutions of (1.1) in which the variables are restricted to a box of points of the type

$$B = \left\{ \underline{x} \in \mathbf{F}_q^n : x_i = \sum_{j=1}^{f} x_{ij}\xi_j,\ a_{ij} \leqslant x_{ij} < a_{ij} + m_{ij},\ 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant f \right\}, \tag{1.2}$$

where $\xi_1, \dots, \xi_f$ is a basis for $\mathbf{F}_q$ over $\mathbf{F}_p$ and a_{ij}, m_{ij} are integers such that $1 \leqslant m_{ij} \leqslant p$ for $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant f$. (Here we have identified $\mathbf{F}_p$ with the set of integers $\{0, 1, \dots, p-1\}$.) See for example Mordell [**Mo1**, **Mo2**], Chalk [**Ch1**, **Ch2**], Chalk and Williams [**CW**], Tietäväinen [**Ti**], R. Smith [**Sm**], Spackman [**Sp**] and Myerson [**My**].

Received by the editors July 12, 1984 and, in revised form, April 15, 1985.
1980 *Mathematics Subject Classification*. Primary 12C15, 10G05, 10B30.
[1] The author was partially supported by a National Science Foundation grant.

In this work we extend the method of Tietäväinen [**Ti**] by viewing it in a new way, in terms of the convolution of finite Fourier series. In so doing we obtain solutions of (1.1) in sets of the form $S + T = \{\underline{s} + \underline{t}\colon \underline{s} \in S, \underline{t} \in T\}$ where S and T are subsets of $\mathbb{F}_q^n$; see Theorem 1.1. We also obtain linearly independent solutions of (1.1) in boxes of sufficiently large cardinality; see Theorem 1.4.

The key ingredient in the investigations mentioned above is a uniform upper bound on the function

$$\phi(V, \underline{y}) = \begin{cases} \sum_{\underline{x} \in V} e(\underline{x} \cdot \underline{y}), & \text{for } \underline{y} \neq \underline{0}, \\ |V| - q^{n-k}, & \text{for } \underline{y} = \underline{0}, \end{cases} \tag{1.3}$$

where $e(\alpha) = e^{(2\pi i/p)\mathrm{Tr}(\alpha)}$ for any $\alpha \in \mathbb{F}_q$, $\underline{x} \cdot \underline{y} = \sum_{i=1}^n x_i y_i$, $\mathrm{Tr}\,\alpha$ is the trace of α from $\mathbb{F}_q$ to $\mathbb{F}_p$ and $|V|$ denotes the cardinality of V. Set $\Phi(V) = \max_{\underline{y} \in \mathbb{F}_q^n} |\phi(V, \underline{y})|$. From Deligne's work on the Riemann Hypothesis, a good bound for $\Phi(V)$ is available if V is suitably nonsingular. To be precise we shall say that a polynomial $f(\underline{x})$ over $\mathbb{F}_q$ is *nonsingular at infinity* over $\mathbb{F}_q$ if its maximal homogeneous part is nonsingular as a form over the algebraic closure of $\mathbb{F}_q$, and that a k-tuple $\underline{F}(\underline{x}) = (f_1(\underline{x}), \ldots, f_k(\underline{x}))$ is "*nonsingular*" *at infinity* over $\mathbb{F}_q$ if every polynomial in the pencil $\{\underline{\lambda} \cdot \underline{F} = \sum_{i=1}^k \lambda_i f_i\colon \underline{\lambda} \in \mathbb{F}_q^k, \underline{\lambda} \neq \underline{0}\}$ is of degree $d \geqslant 2$, $p \nmid d$, and is nonsingular at infinity.

If $\underline{F}(\underline{x})$ is "nonsingular" at infinity then it follows from Theorem 8.4 of Deligne [**De**] and the observation

$$\phi(V, \underline{y}) = q^{-k} \sum_{\substack{\underline{\lambda} \in \mathbb{F}_q^k \\ \underline{\lambda} \neq \underline{0}}} \sum_{\underline{x} \in \mathbb{F}_q^n} e(\underline{\lambda} \cdot \underline{F}(\underline{x}) + \underline{x} \cdot \underline{y})$$

for all $\underline{y}$ in $\mathbb{F}_q^n$, that

$$\Phi(V) \leqslant (d-1)^n q^{n/2}, \tag{1.4}$$

where d is the maximum degree of the polynomials in $\underline{F}(\underline{x})$. In the special case that $g(\underline{x})$ is a quadratic polynomial in an odd number of variables over $\mathbb{F}_q$ and nonsingular at infinity, one can use estimates for Salié sums to improve on (1.4). In this case $\Phi(V(g)) \leqslant 2q^{n/2-1/2}$; see e.g. Carlitz [**Car**].

We can now state our main results.

THEOREM 1.1. *Let S and T be subsets of $\mathbb{F}_q^n$ and V be an algebraic subset of $\mathbb{F}_q^n$ as defined by* (1.1). *Then $(S + T) \cap V$ is nonempty provided that $|S||T| > \Phi^2(V) q^{2k}$.*

This theorem has interesting geometric consequences. For example if we let $q = p$, then (1.1) can be viewed as the system of congruences

$$f_1(\underline{x}) \equiv \cdots \equiv f_k(\underline{x}) \equiv 0 \pmod{p}, \tag{1.5}$$

where now the f_i are taken as polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$. Let B_p be the box in $\mathbb{R}^n$ given by $B_p = \{\underline{x} \in \mathbb{R}^n\colon 0 \leqslant x_i < p, 1 \leqslant i \leqslant n\}$, and again let V be the set of points in $\mathbb{F}_p^n$ satisfying (1.5). We then have

THEOREM 1.2. *If C is a convex subset of B_p containing the origin and the projections of C onto the coordinate planes and* $\mathrm{Vol}(C) > 2^n \Phi(V) p^k$, *then C contains an integral solution of* (1.5).

Of course, since $\Phi(V)$ is invariant under translations and nonsingular linear transformations (mod p), Theorem 1.2 can be applied to a wider class of subsets of $\mathbb{R}^n$. In Corollary 4.1 we state a similar result for any convex subset of $\mathbb{R}^n$ symmetric about a point in $\mathbb{Z}^n$.

Another consequence of Theorem 1.1 is the following

COROLLARY 1.3. *Let B be a box of points in $\mathbb{F}_q^n$ as given by* (1.2) *and V be the set of solutions of* (1.1). *Then $B \cap V$ is nonempty provided that*

$$|B| > 2^{nf}\Phi(V)q^k. \tag{1.6}$$

The corollary follows by applying Theorem 1.1 with

$$S = \left\{ \underline{x} \in \mathbb{F}_q^n\colon x_i = \sum_{j=1}^{f} x_{ij}\xi_j, 0 \leqslant x_{ij} < \left[(m_{ij}+1)/2\right], \right. \\ \left. 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant f \right\} \tag{1.7}$$

and $T = S + \underline{a}$, where $\underline{a} = (\sum_{j=1}^f a_{1j}\xi_j, \dots, \sum_{j=1}^f a_{nj}\xi_j)$, observing that $S + T \subset B$ and that $|S| = |T| \geqslant 2^{-nf}|B|$. When V is defined by a set of polynomials "nonsingular" at infinity this corollary is essentially Myerson's Theorem 2 [**My**]. However, we have eliminated the hypotheses of his theorem that p be sufficiently large and that V be absolutely irreducible over $\mathbb{F}_p$. R. C. Baker [**Ba**, Theorem 2] can improve on Corollary 1.3 in the case that B is centered at the origin, p is sufficiently large and $V = V(f)$, where f is a nonsingular form of degree $\geqslant 3$. He obtains a nontrivial zero $\underline{x}$ of f with $0 < \max_i|x_i| \leqslant p^{1/2+\delta_n+\varepsilon}$ where $\delta_n = 1/(2n-2)$ for $n \geqslant 4$ and $\delta_3 = \frac{1}{6}$.

We shall say that the points $\underline{x}_1, \dots, \underline{x}_n$ in $\mathbb{F}_q^n$ are linearly independent if they are linearly independent as vectors over the field $\mathbb{F}_q$. In order for a subset of $\mathbb{F}_q^n$ to contain n linearly independent points it is necessary that it not be contained in any $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$. On the other hand, if the set is a box we have

THEOREM 1.4. *Let B be a box of points in $\mathbb{F}_q^n$ as given by* (1.2) *and V be the set of solutions of* (1.1). *If B is not contained in any $(n-1)$-dimensional subspace of $\mathbb{F}_q^n$ and $|B| > 4 \cdot 2^{nf}\Phi(V)q^k$, then $B \cap V$ contains n linearly independent points.*

Thus, by increasing the cardinality of B by a factor of 4 we are ensured not only of a solution of (1.1) in B (see (1.6)) but of n linearly independent solutions of (1.1) in B. In particular, if $\underline{F}(\underline{x})$ is "nonsingular" at infinity then there exist n linearly independent solutions $\underline{x} = (x_1, \dots, x_n)$ of $\underline{F}(\underline{x}) = \underline{0}$ with $x_i = \sum_{j=1}^f x_{ij}\xi_j$ and

$$\max_{i,j}|x_{ij}| \leqslant 4^{1/nf}(d-1)^{1/f}p^{1/2+k/n},$$

provided the latter quantity is $< p/2$, where d is the maximum degree of the polynomials in $\underline{F}$.

We wish to thank our thesis director Professor Donald J. Lewis under whom this work was conducted, and Professor Hugh L. Montgomery for his comments and suggestion in proving Lemma 5.1. We also wish to thank the referee for many helpful comments on preparing this paper. This work was submitted as a portion of the author's doctoral thesis at the University of Michigan.

2. Method of proof, finite Fourier series. Throughout the paper we shall abbreviate "complete" sums $\sum_{\underline{x} \in \mathbb{F}_q^n}(\ )$ by just $\sum_{\underline{x}}(\ )$. Let S be a subset of $\mathbb{F}_q^n$ and V be an algebraic subset of $\mathbb{F}_q^n$ as defined by (1.1). Let $\alpha(\underline{x})$ be a real valued function on $\mathbb{F}_q^n$ such that $\alpha(\underline{x}) \leqslant 0$ for all $\underline{x}$ not in S, and $\sum_{\underline{x}}\alpha(\underline{x}) > 0$. In order to show $S \cap V$ is nonempty it suffices to choose $\alpha(\underline{x})$ so that $\sum_{\underline{x} \in V}\alpha(\underline{x}) > 0$. Now $\alpha(\underline{x})$ has a finite Fourier expansion $\alpha(\underline{x}) = \sum_{\underline{y}} a(\underline{y})e(\underline{y} \cdot \underline{x})$, where $a(\underline{y}) = q^{-n}\sum_{\underline{x}}\alpha(\underline{x})e(-\underline{y} \cdot \underline{x})$ for $\underline{y} \in \mathbb{F}_q^n$. Thus

$$\begin{aligned}\sum_{\underline{x} \in V} \alpha(\underline{x}) &= \sum_{\underline{x} \in V} \sum_{\underline{y}} a(\underline{y})e(\underline{y} \cdot \underline{x}) \\ &= a(\underline{0})|V| + \sum_{\underline{y} \neq \underline{0}} a(\underline{y}) \sum_{\underline{x} \in V} e(\underline{y} \cdot \underline{x}) \\ &= a(\underline{0})q^{n-k} + a(\underline{0})\left(|V| - q^{n-k}\right) + \sum_{\underline{y} \neq \underline{0}} a(\underline{y})\phi(V, \underline{y})\end{aligned}$$

and so,

$$\sum_{\underline{x} \in V} \alpha(\underline{x}) = q^{-k}\sum_{\underline{x}}\alpha(\underline{x}) + \sum_{\underline{y}} a(\underline{y})\phi(V, \underline{y}). \tag{2.1}$$

Equation (2.1) expresses the "incomplete" sum $\sum_{\underline{x} \in V}\alpha(\underline{x})$ as a fraction of the "complete" sum $\sum_{\underline{x}}\alpha(\underline{x})$ plus an error term. In §5 we consider the problem of making an optimal choice of $\alpha(\underline{x})$ in order to minimize the error term.

The idea of Tietäväinen **[Ti]** which has since been used by Chalk **[Ch2]** and Myerson **[My]** was to count the number of ways of expressing points in V as the sum of points from subsets S and T of $\mathbb{F}_q^n$. This can be viewed as a special case of (2.1), taking $\alpha(\underline{x})$ as the convolution of χ_S and χ_T, the characteristic functions of S and T respectively. Chalk's equation (15) **[Ch2]** is a variation of (2.1) for this choice of $\alpha(\underline{x})$. We recall that if $\alpha(\underline{x})$ and $\beta(\underline{x})$ are complex valued functions on $\mathbb{F}_q^n$, then their convolution, written $\alpha * \beta$, is defined by

$$\alpha * \beta(\underline{x}) = \sum_{\underline{u}} \alpha(\underline{u})\beta(\underline{x} - \underline{u}) = \sum_{\underline{u} + \underline{v} = \underline{x}} \alpha(\underline{u})\beta(\underline{v}) \quad \text{for } \underline{x} \in \mathbb{F}_q^n.$$

If H is an additive subgroup of $\mathbb{F}_q^n$ we define its orthogonal space $H^{\perp}$ as follows:

$$H^{\perp} = \left\{\underline{x} \in \mathbb{F}_q^n \colon \mathrm{Tr}(\underline{x} \cdot \underline{y}) = 0 \text{ for all } \underline{y} \in H\right\}.$$

Using the fact that $\mathbb{F}_q^n = H \oplus H^{\perp}$ one can easily deduce that the Fourier coefficients $a_H(\underline{y})$ of χ_H are given by

$$a_H(\underline{y}) = \begin{cases} q^{-n}|H| & \text{if } \underline{y} \in H^{\perp}, \\ 0 & \text{if } \underline{y} \notin H^{\perp}. \end{cases}$$

Thus

$$\sum_{\underline{y}} \left|a_H(\underline{y})\right| = 1. \tag{2.2}$$

3. Proofs of Theorems 1.1 and 1.4. Let S and T be subsets of $\mathbb{F}_q^n$ and H be an additive subgroup of $\mathbb{F}_q^n$. The proofs of Theorems 1.1 and 1.4 are based on the following identity:

$$\sum_{\underline{x}\in H\cap V} \chi_S * \chi_T(\underline{x}) = q^{-k} \sum_{\underline{x}\in H} \chi_S * \chi_T(\underline{x}) + \theta\Phi(V)|S|^{1/2}|T|^{1/2} \tag{3.1}$$

for some θ with $|\theta| \leqslant 1$. To obtain (3.1) we use equation (2.1) with $\alpha(\underline{x}) = (\chi_S * \chi_T) \cdot \chi_H(\underline{x})$. It suffices to show that the error term in (2.1) is less than $\Phi(V)|S|^{1/2}|T|^{1/2}$ in absolute value, and so it is enough to show that $\sum_{\underline{y}}|a(\underline{y})| \leqslant |S|^{1/2}|T|^{1/2}$. Let $a_H(\underline{y})$, $a_S(\underline{y})$ and $a_T(\underline{y})$ be the Fourier coefficients of χ_H, χ_S and χ_T respectively. Then by elementary properties of Fourier coefficients, $a(\underline{y}) = q^n((a_S \cdot a_T) * a_H)(\underline{y})$, and so by (2.2) we have

$$\begin{aligned}\sum_{\underline{y}}|a(\underline{y})| &\leqslant q^n \sum_{\underline{y}} |(a_S\cdot a_T)(\underline{y})| \cdot \sum_{\underline{y}} |a_H(\underline{y})| \\ &= q^n \sum_{\underline{y}} |a_S(\underline{y})|\,|a_T(\underline{y})| \\ &\leqslant q^n\Big(\sum_{\underline{y}}|a_S(\underline{y})|^2\Big)^{1/2}\Big(\sum_{\underline{y}}|a_T(\underline{y})|^2\Big)^{1/2}.\end{aligned}$$

Using Parseval's identity we deduce that

$$\begin{aligned}\sum_{\underline{y}}|a(\underline{y})| &\leqslant q^n\Big(q^{-n}\sum_{\underline{x}}|\chi_S(\underline{x})|^2\Big)^{1/2}\Big(q^{-n}\sum_{\underline{x}}|\chi_T(\underline{x})|^2\Big)^{1/2} \\ &= |S|^{1/2}|T|^{1/2}.\end{aligned}$$

To prove Theorem 1.1 we apply (3.1) with $H = \mathbb{F}_q^n$, yielding

$$\sum_{\underline{x}\in V} \chi_S * \chi_T(\underline{x}) \geqslant q^{-k}|S|\,|T| - \Phi(V)|S|^{1/2}|T|^{1/2}. \tag{3.2}$$

The left-hand side of (3.2) is positive provided that $|S|\,|T| > \Phi^2(V)q^{2k}$.

Theorem 1.4 follows from the following proposition. For any subsets S, T and H of $\mathbb{F}_q^n$ we set

$$N(H,S,T) = \sum_{\underline{x}\in H} \chi_S * \chi_T(\underline{x}) = |\{(\underline{s},\underline{t}) \in S \times T\colon \underline{s} + \underline{t} \in H\}|.$$

PROPOSITION 3.1. *Let S and T be subsets of $\mathbb{F}_q^n$ and V be an algebraic subset of $\mathbb{F}_q^n$ as given by* (1.1). *Suppose κ is a number less than one such that for every $(n-1)$-dimensional subspace H of $\mathbb{F}_q^n$, $N(H,S,T) \leqslant \kappa|S|\,|T|$. Then $(S+T)\cap V$ contains n linearly independent points provided that*

$$|S|\,|T| > \Big(\frac{2}{1-\kappa}\Big)^2 \Phi^2(V)q^{2k}.$$

PROOF. Suppose that $(S+T)\cap V$ contains no more than $(n-1)$ linearly independent points. Then there exists an $(n-1)$-dimensional subspace H such that $(S+T)\cap V \subset H$, which implies that

$$\sum_{\underline{x}\in H\cap V} \chi_S * \chi_T(\underline{x}) = \sum_{\underline{x}\in V} \chi_S * \chi_T(\underline{x}).$$

Therefore, by (3.1) and our assumption on $N(H, S, T)$,

$$\sum_{\underline{x} \in V} \chi_S * \chi_T(\underline{x}) \leqslant \kappa q^{-k}|S||T| + \Phi(V)|S|^{1/2}|T|^{1/2}.$$

Hence, by (3.2) we conclude that

$$|S||T| \leqslant \left(\frac{2}{1-\kappa}\right)^2 \Phi^2(V) q^{2k}.$$

Proof of Theorem 1.4. We simply apply the proposition to the boxes S and T as defined by (1.7). It suffices to show that κ can be taken as $\frac{1}{2}$. Let H be an $(n-1)$-dimensional subset of $\mathbb{F}_q^n$. Without loss of generality we may assume that H is the zero set of a linear equation $\sum_{i=1}^r a_i x_i = 0$, where $1 \leqslant r \leqslant n$ and $a_i \neq 0$ for $1 \leqslant i \leqslant r$. The quantity $N(H, S, T)$ is the number of $(\underline{s}, \underline{t})$ in $S \times T$ such that $\sum_{i=1}^r a_i(s_i + t_i) = 0$. Now, S and T can be written as $S = S_1 \times \cdots \times S_n$ and $T = T_1 \times \cdots \times T_n$. If $|S_i| > 1$ or $|T_i| > 1$ for some i with $1 \leqslant i \leqslant r$, then on solving for s_i or t_i respectively in the above equation we see that $N(H, S, T) \leqslant \frac{1}{2}|S||T|$. Thus we may suppose that $S_i = \{\sigma_i\}$ and $T_i = \{\tau_i\}$ for some σ_i, $\tau_i \in \mathbb{F}_q$, $1 \leqslant i \leqslant r$. Since $(S + T) \not\subset H$ it follows that $N(H, S, T) = 0$ in this case.

4. Geometric consequences of Theorem 1.1. Let $\underline{F}(\underline{x})$ be a k-tuple of polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ and p be a prime. We define $V = V(\underline{F})$ and $\Phi(V)$ as in §1, reading the polynomials in $\underline{F}(\underline{x})$ modulo p. For any subset S of $\mathbb{Z}^n$ let $|\hat{S}|$ denote the number of distinct points in S (mod p), that is $|\hat{S}| = |(S + p\mathbb{Z}^n)/p\mathbb{Z}^n|$. Theorem 1.1 now says that for any subsets S and T of $\mathbb{Z}^n$, $S + T$ contains a solution of (1.5) provided that $|\hat{S}||\hat{T}| > \Phi^2(V)p^{2k}$. In particular if we let C be any convex subset of $\mathbb{R}^n$ and let $S = \frac{1}{2}C \cap \mathbb{Z}^n = \{\underline{x} \in \mathbb{Z}^n \colon 2\underline{x} \in C\}$, then C contains an integral solution of (1.5) provided that $|\hat{S}| > \Phi(V)p^k$. This follows by taking $T = S$ and observing that $S + T \subset \frac{1}{2}C + \frac{1}{2}C \subset C$.

Proof of Theorem 1.2. Let C be a convex subset of B_p containing the origin and the projections of C onto the coordinate planes. It is easy to see that for any $\underline{x}$ in C, C contains the set of $\underline{y}$ in $\mathbb{R}^n$ such that $0 \leqslant y_i \leqslant x_i$ for $1 \leqslant i \leqslant n$. Let $S = \frac{1}{2}C \cap \mathbb{Z}^n$ and let D be the unit box $D = \{\underline{x} \in \mathbb{R}^n \colon 0 \leqslant x_i < 1, 1 \leqslant i \leqslant n\}$. We know $\frac{1}{2}C \subset \bigcup_{\underline{s} \in S}(\underline{s} + D)$, for if $\underline{x} \in \frac{1}{2}C$ then $\underline{y} = ([x_1], [x_2], \ldots, [x_n]) \in \frac{1}{2}C \cap \mathbb{Z}^n = S$ and $\underline{x} \in \underline{y} + D$. Thus $\mathrm{Vol}(\frac{1}{2}C) \leqslant |S| = |\hat{S}|$ and so it suffices to take $\mathrm{Vol}(C) \geqslant 2^n\Phi(V)p^k$ in order for C to contain a solution of (1.5).

For any $\underline{x} \in \mathbb{R}^n$ let $\|\underline{x}\| = \max_{i=1,\ldots,n}|x_i|$, and for any subset S of $\mathbb{R}^n$ let $\|S\| = \sup_{\underline{x}, \underline{y} \in S}\|\underline{x} - \underline{y}\|$.

Corollary 4.1. *Let C be a convex subset of $\mathbb{R}^n$ symmetric about a point $\underline{z}$ in $\mathbb{Z}^n$ such that $\|C\| < 2p$ and*

$$\mathrm{Vol}(C) > 2^{2n-1}(\Phi(V)p^k + 1). \tag{4.1}$$

Then C contains a solution of (1.5).

Proof. Since $\Phi(V)$ is invariant under translations, we may assume that $\underline{z} = \underline{0}$. Let $S = \frac{1}{2}C \cap \mathbb{Z}^n$ and suppose $\mathrm{Vol}(C)$ satisfies (4.1). Then

$$\mathrm{Vol}(\tfrac{1}{2}C) > 2^n(\tfrac{1}{2}\Phi(V)p^k + \tfrac{1}{2}),$$

and so by a generalized version of Minkowski's fundamental theorem (see [**Cas**, Theorem II, p. 71]), $\frac{1}{2}C$ contains at least $\Phi(V)p^k$ distinct lattice points. But as $\|\frac{1}{2}C\| < p$, this implies that $|\hat{S}| > \Phi(V)p^k$ and so C contains a solution of (1.5).

5. Best possible choices for $\alpha(\underline{x})$. Let S, V and $\alpha(\underline{x})$ be as defined in §2, where without loss of generality $\alpha(\underline{x})$ is taken so that $\sum_{\underline{x}}\alpha(\underline{x}) = 1$. We now seek the optimal choice of $\alpha(\underline{x})$ in order to show $S \cap V$ is nonempty, that is, $\sum_{\underline{x}\in V}\alpha(\underline{x}) > 0$. This amounts to minimizing the error term

$$E(V,\alpha) = \sum_{\underline{y}} a(\underline{y})\phi(V,\underline{y})$$

in equation (2.1). If we bound $E(V,\alpha)$ by saying

$$|E(V,\alpha)| \leqslant \Phi(V)\sum_{\underline{y}}|a(\underline{y})|, \tag{5.1}$$

then the problem becomes one of minimizing $\sum_{\underline{y}}|a(\underline{y})|$, a quantity which depends only on the pair S, $\alpha(\underline{x})$ and not on V. The following lemma gives us a lower bound on this quantity.

LEMMA 5.1. *Let $\alpha(\underline{x})$ be a real valued function on $\mathbb{F}_q^n$ such that $\alpha(\underline{x}) \leqslant 0$ for $\underline{x} \notin S$, $\sum_{\underline{x}}\alpha(\underline{x}) = 1$ and $\alpha(\underline{x}) = \sum_{\underline{y}}a(\underline{y})e(\underline{x}\cdot\underline{y})$. Then $\sum_{\underline{y}}|a(\underline{y})| \geqslant |S|^{-1}$.*

PROOF. For any subset W of $\mathbb{F}_q^n$ it follows from the assumption $\sum_{\underline{x}}\alpha(\underline{x}) = 1$ that

$$\sum_{\underline{x}\in W}\alpha(\underline{x}) = q^{-n}|W| + \sum_{\underline{y}\neq\underline{0}} a(\underline{y})\phi(W,\underline{y}), \tag{5.2}$$

where as before $\phi(W,\underline{y}) = \sum_{\underline{x}\in W}e(\underline{x}\cdot\underline{y})$ for $\underline{y} \neq \underline{0}$. If we take W to be the complement of S in $\mathbb{F}_q^n$, then for $\underline{y} \neq \underline{0}$, $\phi(W,\underline{y}) = \sum_{\underline{x}}e(\underline{x}\cdot\underline{y}) - \sum_{\underline{x}\in S}e(\underline{x}\cdot\underline{y}) = -\sum_{\underline{x}\in S}e(\underline{x}\cdot\underline{y})$, and so $|\phi(W,\underline{y})| \leqslant |S|$. Since $W \cap S = \varnothing$, we deduce from (5.2) that

$$0 \geqslant \sum_{\underline{x}\in W}\alpha(\underline{x}) \geqslant q^{-n}|W| - |S|\sum_{\underline{y}\neq\underline{0}}|a(\underline{y})| = 1 - |S|\sum_{\underline{y}}|a(\underline{y})|,$$

and the conclusion follows.

If S is a box of points as given by (1.2), then the lower bound in Lemma 5.1 can be obtained, up to a factor of 2^{nf}. This is seen by taking $\alpha(\underline{x}) = |T|^{-1}|U|^{-1}\chi_T * \chi_U(\underline{x})$, where U and T are boxes as given by (1.7). As we saw in deriving equation (3.1), $\sum_{\underline{y}}|a(\underline{y})| \leqslant |T|^{-1/2}|U|^{-1/2} \leqslant 2^{nf}|B|^{-1}$. Thus the only improvement that can be made in Corollary 1.3 if we use a bound of the type (5.1) is a savings of a factor of 2^{nf} in (1.6).

REFERENCES

[**Ba**] R. C. Baker, *Small solutions of congruences*, Mathematika **30** (1983), 164–188.

[**Car**] L. Carlitz, *Weighted quadratic partitions over a finite field*, Canad. J. Math. **5** (1953), 317–323.

[**Cas**] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, Berlin, 1959.

[**Ch1**] J. H. H. Chalk, *The number of solutions of congruences in incomplete residue systems*, Canad. J. Math. **15** (1963), 291–296.

[**Ch2**] ______, *The Vinogradov-Mordell-Tietäväinen inequalities*, Indag. Math. **42** (1980), 367–374.

[**CW**] J. H. H. Chalk and K. S. Williams, *The distribution of solutions of congruences*, Mathematika **12** (1965), 176–192.

[**De**] P. Deligne, *La conjecture de Weil*. I, Publ. Math. IHES **43** (1974), 273–307.

[**Mo1**] L. J. Mordell, *The number of solutions in incomplete residue sets of quadratic congruences*, Arch. Math. **8** (1957), 153–157.

[**Mo2**] ______, *Incomplete exponential sums and incomplete residue systems for congruences*, Czechoslovak. Math. J. **14** (1964), 235–242.

[**My**] G. Myerson, *The distribution of rational points on varieties defined over a finite field*, Mathematika **28** (1981), 153–159.

[**Sm**] R. A. Smith, *The distribution of rational points on hypersurfaces defined over a finite field*, Mathematika **17** (1970), 328–332.

[**Sp**] K. Spackman, *On the number and distribution of simultaneous solutions to diagonal congruences*, Canad. J. Math. **33** (1981), 421–436.

[**Ti**] A. Tietäväinen, *On the solvability of equations in incomplete finite fields*, Ann. Univ. Turku. Ser. AI **102** (1967), 1–13.

Department of Mathematics, Kansas State University, Manhattan, Kansas 66506